0418017-SNY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212454
(43)Date of publication of application : 06.08.1999

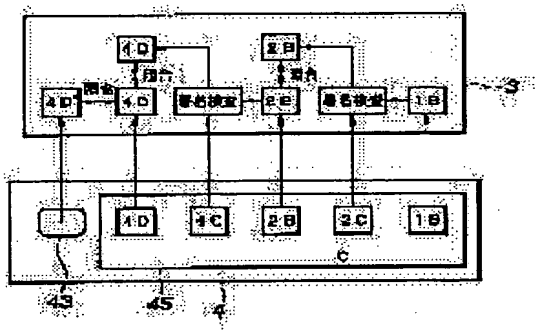
(51)Int.Cl. G09C 1/00
G11B 20/10

(21)Application number : 10-015666
(22)Date of filing : 28.01.1998

(71)Applicant : MATSUMOTO TSUTOMU
NHK SPRING CO LTD
(72)Inventor : MATSUMOTO TSUTOMU
MATSUMOTO HIROYUKI
YAMAMOTOYA KENJI

(54) AUTHENTICATION TYPE SECURITY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To effectively prevent an authenticated body from being forged, to facilitate the maintenance, and to evade complexity of the structure of, specially, the authenticated body side by collating feature data with physical features which are read at the time of authentication and deciding whether or not the authenticated body is genuine or false according to the respective matching results.
SOLUTION: When a card 4 to be authenticated is inserted into a card reader 3, issue device sign data 4c, feature data 4C, etc., stored on a magnetic stripe 45 are read out and physical features are read as feature data 4D' out of a reference area 43 along a read track set on the card reader 3. The authentication device sign data 2C are deciphered with authentication device open key data 1B and collated with issue device open key data 2B. Issue device sign data 4C are deciphered with the issue device open key data 2B and collated with feature data 4D. The feature data 4D' and feature data 4D are collated with each other. When the respective collated results meet specific conditions, it is decided that the card 4 is a regular card.



LEGAL STATUS

[Date of request for examination] 07.08.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－212454

(43)公開日　平成11年(1999)８月６日

(51)Int.Cl.⁶	識別記号	FI	
G09C 1/00	640	G09C 1/00	640B
			640D
G11B 20/10		G11B 20/10	H

審査請求　未請求　請求項の数８　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－15666

(22)出願日　平成10年(1998)１月28日

(71)出願人　596048536
松本　勉
神奈川県横浜市青葉区柿の木台13番地45

(71)出願人　000004640
日本発条株式会社
神奈川県横浜市金沢区福浦３丁目10番地

(72)発明者　松本　勉
神奈川県相模原市上鶴間2603－１　サンヴェール町田グランデュール210

(72)発明者　松本　弘之
神奈川県横浜市金沢区福浦３丁目10番地
日本発条株式会社内

(74)代理人　弁理士　大島　陽一

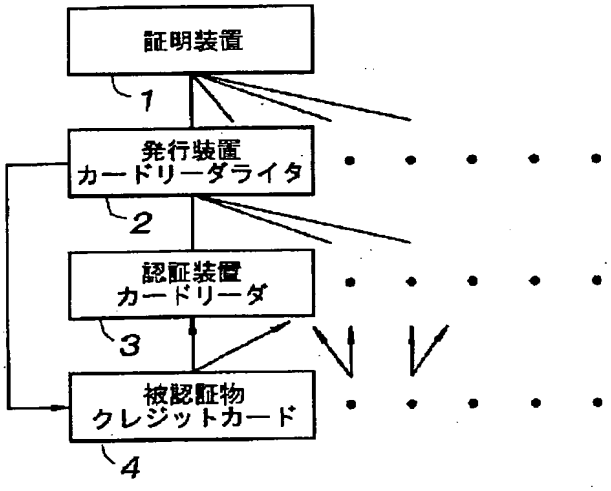
最終頁に続く

(54)【発明の名称】　認証式セキュリティシステム

(57)【要約】

【課題】　被認証物の偽造を防止し得ると共に保守が容易であり、特に被認証物側の構造も複雑化することのないセキュリティシステムを提供する。

【解決手段】　基準領域の物理的特徴データ、この特徴データを発行装置用秘密鍵データにより暗号化した署名データ及び発行装置用公開鍵データを被認証物のデータ格納領域に格納し、これを認証時に読み出すと共にその基準領域の特徴を読み取り、これらの照合結果により被認証物の真正性を確認可能としたため、秘密鍵データを知らずに署名データを解析することは困難であり、また被認証物に格納されたデータを単にデッドコピーしても他の被認証物では基準領域の特徴が異なることからその真正性は否定されるため他の被認証物への不正な適用をも防止でき、しかも認証に必要なデータが全て被認証物側にあることから、認証装置側の記憶容量を著しく低減でき、また秘密鍵・公開鍵データの変更、追加しても認証装置側の更新を必要とせずその保守が簡便になる。



【特許請求の範囲】

【請求項１】　証明装置が証明した発行装置が発行した被認証物を認証装置をもって認証することでその真正性の判定行い、前記被認証物の偽造を防止するためのセキュリティシステムであって、

前記被認証物が、機械により読み取り可能であるが、無作為に生成されているために人為的に同一なものを製作することが困難な物理的特徴を有する基準領域と、発行時に前記基準領域から読み取った特徴データ、該特徴データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる発行装置署名データ及び前記発行装置署名データを復号するための発行装置用公開鍵データを記憶保持するためのデータ格納領域とを有し、

認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された特徴データ、発行者署名データ及び発行装置用公開鍵データを読み出すと共に前記基準領域からその物理的特徴を読み取り、

前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、

前記特徴データと、認証時に読み取った物理的特徴とを照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする認証式セキュリティシステム。

【請求項２】　前記被認証物が、連続するまたは不連続な複数の基準領域を有し、かつ前記データ格納領域が、前記各基準領域に対応する特徴データ及びそれに対応する発行装置署名データを記憶保持するようになっており、

認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された発行装置用公開鍵データを読み出すと共に選択的に１つまたは複数の特徴データ及びそれに対応する発行装置署名データを読み出し、更に前記読み出した特徴データに対応する基準領域からその物理的特徴を読み取り、

前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、

前記特徴データと、認証時に読み取った物理的特徴とを照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項１に記載の認証式セキュリティシステム。

【請求項３】　前記被認証物が、演算処理部を更に有し、かつ前記データ格納領域が、被認証物毎に設定される被認証物用秘密鍵データ、被認証物用公開鍵データ及び前記被認証物用公開鍵データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる別の発行装置署名データを更に記憶保持するようになっており、

認証時に、前記データ格納領域から被認証物用公開鍵データ及び前記別の発行装置署名データをも更に読み出し、

前記発行装置用公開鍵データをもって前記被認証物署名データを復号して前記被認証物用公開鍵データと照合し、

前記認証装置から認証の度に異なる確認データを前記被認証物に送り、その前記演算処理部にて前記被認証物用秘密鍵データにより前記確認データを暗号化して前記認証装置に送り返し、該認証装置にて前記被認証物用公開鍵データをもって復号して前記確認データと照合し、

前記特徴データと、認証時に読み取った物理的特徴とを照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項１または請求項２のいずれかに記載の認証式セキュリティシステム。

【請求項４】　前記確認データが認証時に読み取った物理的特徴に基づき生成されるようになっていることを特徴とする請求項３に記載の認証式セキュリティシステム。

【請求項５】　前記被認証物の前記データ格納領域が、前記発行装置用公開鍵データを前記証明装置にて証明装置用秘密鍵データにより暗号化してなる証明装置署名データ及び前記証明装置用秘密鍵データにより暗号化された証明装置署名データを復号するための証明装置用公開鍵データをも更に格納するようになっており、

認証時に前記証明装置署名データ及び前記証明装置用公開鍵データをも読み出し、

前記証明装置用公開鍵データをもって前記証明装置署名データを復号したものと前記発行装置用公開鍵データとを更に照合し、

前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項１乃至請求項４のいずれかに記載の認証式セキュリティシステム。

【請求項６】　前記認証装置が前記証明装置と接続可能となっており、かつ過去の認証時に被認証物から読み出された証明装置用公開鍵データを１つまたは２つ以上記憶可能となっており、

認証時に被認証物から読み出された証明装置用公開鍵データを記憶された証明装置用公開鍵データと比較し、一致すれば該証明装置用公開鍵データを用いて前記照合を行い、一致しなければ前記証明装置に問い合わせて正規の証明装置用公開鍵データであることが確認されたら該証明装置用公開鍵データを用いて前記照合を行うと共にこれを記憶するようになっていることを特徴とする請求項５に記載の認証式セキュリティシステム。

【請求項７】　前記被認証物の前記データ格納領域が、前記発行装置用公開鍵データを前記証明装置にて証明装置用秘密鍵データにより暗号化してなる証明装置署名データをも更に格納するようになっており、

前記認証装置が、前記証明装置用秘密鍵データにより暗号化された証明装置署名データを復号するための証明装置用公開鍵データを記憶しており、
認証時に前記証明装置署名データをも読み出し、
前記証明装置用公開鍵データをもって前記証明装置署名データを復号したものと前記発行装置用公開鍵データとを更に照合し、
前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする請求項１乃至請求項４のいずれかに記載の認証式セキュリティシステム。
【請求項８】　前記基準領域が、紙または樹脂中に磁性体繊維を無作為に配置したものからなることを特徴とする請求項１乃至請求項７のいずれかに記載の認証式セキュリティシステム。
【発明の詳細な説明】
【０００１】
【発明が属する技術分野】本発明は、例えばプリペイドカード、クレジットカード、ＩＤカードなどの真正性の判定を要する被認証物の偽造を防止するためのセキュリティシステムに関する。
【０００２】
【従来の技術】従来のセキュリティーシステムの１つの手法として、証明装置（機関）と、発行装置（機関）とにより、秘密鍵データによる署名生成ルールを用いて元のデータから署名データを生成し、これをクレジットカード等の被認証物に例えば磁気記録し、該被認証物を発行し、認証装置に記憶された公開鍵データから署名検査ルールを用いて上記署名データを検査してこの被認証物を認証することによりその真正性を確認する認証システムが知られている。
【０００３】このシステムによれば、署名生成ルールを知る者のみが、自らの署名データを新たに生成したり、当該データを改変することができるこから、新たな被認証物を装う偽造行為に対する防止効果は高いものの、例えば認証装置と被認証物との間の通信を傍受したり被認証物から署名データを読み出してデッドコピーすることによる不正は防止できない。
【０００４】一方、被認証物の偽造や複製を防止する手段として、例えばその被認証物に固有の物理的な特徴をデータとして記録し、このデータと実際の物理的な特徴とを照合して真正性を判定する方法も提案されている。
【０００５】そこで、本願出願人は、例えば特願平８－８５９４６号明細書に記載されているように、各被認証物毎の物理的な特徴データを上記署名データとしてその被認証物に記録し、認証時に被認証物の物理的特徴を読み取ると共にこの署名データを特徴データに戻して両者を比較する方法を提案した。
【０００６】この方法によれば、被認証物の記録内容を知ってもその被認証物毎の物理的な特徴をも模倣しない限り偽造することはできないことからその偽造防止効果は著しく高くなる。
【０００７】
【発明が解決しようとする課題】しかしながら、上記証明装置と、発行装置とが同一であり、かつこれらと認証装置とが一対一対応であれば良いが、例えばクレジットカードの場合、通常、証明装置（クレジット会社）と、発行装置（クレジット会社、銀行等）とは同一の機関である可能性はあるもののこれらとクレジットカードを使用する店などに設置される認証装置とは別々の機関であることが多く、特に発行装置に比較して認証装置が著しく多い。従って、上記秘密鍵データや公開鍵データを変更する場合や発行装置（機関）が増減する場合、その度に各認証装置に記憶された公開鍵データ等を変更しなければならず、その保守が厄介であった。
【０００８】一方、被認証物側にＩＣによる演算処理部を設け、認証の度に認証装置から被認証物に乱数等の確認データを秘密鍵データにより生成した署名データを送り、これを公開鍵データにより元の確認データに戻して送り返す動作を付加し、認証装置と被認証物側との間の通信内容を認証の度に変える動的認証方法も提案されているが、被認証物側で複雑な計算を行わなければならないことから、そのためのＩＣが大型化、高騰化する問題があった。
【０００９】このような従来技術の問題に鑑み、本発明の主な目的は、被認証物の偽造を効果的に防止し得ると共に保守が容易であり、特に被認証物側の構造も複雑化することのないセキュリティシステムを提供することにある。
【００１０】
【課題を解決するための手段】上記の目的は本発明によれば、発行装置が発行し、かつ証明装置が証明した被認証物を認証装置をもって認証することでその真正性の判定行い、前記被認証物の偽造を防止するためのセキュリティシステムであって、前記被認証物が、機械により読み取り可能であるが、無作為に生成されているために人為的に同一なものを製作することが困難な物理的特徴を有する基準領域と、発行時に前記基準領域から読み取った特徴データ、該特徴データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる発行装置署名データ及び前記発行装置用秘密鍵データにより暗号化された発行装置署名データを復号するための発行装置用公開鍵データを記憶保持するためのデータ格納領域とを有し、認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された特徴データ、発行装置署名データ及び発行装置用公開鍵データを読み出すと共に前記基準領域からその物理的特徴を読み取り、前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、前記特徴データと、認証時に読み取った物理的特徴とを照合し、前記各照合結果に基

づき前記被認証物の真正性の判定が行われるようになっていることを特徴とする認証式セキュリティシステムを提供することにより達成される。また、前記被認証物が、連続するまたは不連続な複数の基準領域を有し、かつ前記データ格納領域が、前記各基準領域に対応する特徴データ及びそれに対応する発行装置署名データを記憶保持するようになっており、認証時に、前記認証装置にて前記被認証物のデータ格納領域に格納された発行装置用公開鍵データを読み出すと共に選択的に１つまたは複数の特徴データ及びそれに対応する発行装置署名データを読み出し、更に前記読み出した特徴データに対応する基準領域からその物理的特徴を読み取り、前記発行装置用公開鍵データをもって前記発行装置署名データを復号して前記特徴データと照合し、前記特徴データと、認証時に読み取った物理的特徴とを照合し、前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていると良く、更に、前記被認証物が、演算処理部を更に有し、かつ前記データ格納領域が、被認証物毎に設定される被認証物用秘密鍵データ、被認証物用公開鍵データ及び前記被認証物用公開鍵データを前記発行装置にて発行装置用秘密鍵データにより暗号化してなる別の発行装置署名データを更に記憶保持するようになっており、認証時に、前記データ格納領域から被認証物用公開鍵データ及び前記別の発行装置署名データをも読み出し、前記発行装置用公開鍵データをもって前記被認証物署名データを復号して前記被認証物用公開鍵データと照合し、前記認証装置から認証の度に異なる確認データを前記被認証物に送り、その前記演算処理部にて前記被認証物用秘密鍵データにより前記確認データを暗号化して前記認証装置に送り返し、該認証装置にて前記被認証物用公開鍵データをもって復号して前記確認データと照合し、前記特徴データと、認証時に読み取った物理的特徴とを照合し、前記各照合結果に基づき前記被認証物の真正性の判定が行われるようになっていると良い。

【００１１】このようにすれば、秘密鍵データを知らずに署名データを解析することは著しく困難であり、また被認証物のデータ格納領域に格納されたデータを単にデッドコピーしても他の被認証物では基準領域の特徴が異なることからその真正性は否定されるため他の被認証物への不正な適用をも効果的に防止することができ、しかも認証に必要なデータが全て被認証物側にあることから、発行装置用秘密鍵データや発行装置用公開鍵データを変更したり新たな発行装置用秘密鍵データや発行装置用公開鍵データを追加しても認証装置側の更新を必要としない。

【００１２】特に、認証の度に被認証物と認証装置との通信内容を変えるようにする場合、請求項２のように被認証物側に格納された複数のデータの１つまたは幾つかを認証装置側で選択して読み出すようにすることで、被認証物側に演算処理のための１Ｃ等を設ける必要がなく、しかも処理が簡便になる。

【００１３】基準領域として、紙又は樹脂中に磁性体繊維を無作為に配置したものや、紙の漉きむらを利用したり、シート材の表面粗さなど、人為的に複製することが困難で、しかも所定の機械では再現性良く検出し得るものであれば、任意のものを用いることができる。そのような例としては、特開平６－１６８３６３号、特開昭５２－３３４４４号、特表昭５７－５００８５１号の各公報に開示されたものなどがある。

【００１４】

【発明の実施の形態】以下、本発明の好適実施形態を添付の図面について詳しく説明する。

【００１５】図１は、本発明が適用された第１の実施形態における認証式セキュリティシステムの概略構成を示すブロック図である。このシステムは、クレジットカードにおける認証式セキュリティシステムであり、証明装置１が１つまたは複数設置された証明機関（カード会社）と、カードの発行装置としてのカードリーダライタ２が１つまたは複数設置された発行機関（銀行、代理店等）と、認証装置としてのカードリーダ３が１つまたは複数設置された認証者（カードを使用する店、施設等）と、通常は多数発行される被認証物としてのクレジットカード４とから構成される。

【００１６】図２は、クレジットカード４を示す平面図であり、このクレジットカード４はポリエステル製のベースシート４１からなり、このカードには、発行者、券種やカードの使途を特定するために必要な管理データとは別に、後記する特徴データ、発行装置署名データ、発行装置用公開鍵データ、証明装置署名データ及び証明装置用公開鍵データを格納するための識別データ格納領域を含む磁気ストライプ４２と、磁性体繊維をベースシート４１の樹脂中に無作為に分散してなる基準領域４３とが設けられている。

【００１７】図３は、本発明が適用された発行装置としてのカードリーダライタ２を示す。カードリーダライタ２は、カードをスロット２１内に取り込み、データ書き込み後にカードを排出するためのモータ駆動されたローラを含むカード搬送ユニット２２が内蔵されている。スロット２１に沿って、磁気ストライプ４２から磁気データを読み出し／書き込みするための磁気ヘッド２３及び基準領域４３を読み取るための誘導式磁気ヘッド２４が設けられている。磁気ヘッド２３、２４はその入出力を制御すると共にデータ処理を行うための制御ユニット２５に接続されている。尚、実際に発行されたカードを認証するための認証装置としてのカードリーダ３は書き込み機能を除き、カードリーダライタ２と同様であるのでその詳細な説明を省略する。

【００１８】以下に、図４～図６に沿ってカード４の発行手順及び認証手順を説明する。証明装置１は、証明装置用秘密鍵データ１Ａを用いて特定の署名生成ルールに

より各発行装置用公開鍵データ２Ｂを暗号化して証明装置署名データ２Ｃを生成するようになっている。この証明装置署名データ２Ｃは証明装置用公開鍵データ１Ｂを用いた特定の署名検査ルールによってのみ復号し得る。同様に、カードリーダライタ２の制御ユニット２５は、発行装置用秘密鍵データ２Ａを用いた上記同様な署名生成ルールにより各カード４の後記する特徴データ４Ｄを暗号化して発行装置署名データ４Ｃを生成するようになっている。この発行装置署名データ４Ｃは発行装置用公開鍵データ２Ｂを用いた上記同様な署名検査ルールによってのみ復号し得る。

【００１９】まず、図４に示すように、準備段階として、発行装置としてのカードリーダライタ２に、発行装置用秘密鍵データ２Ａ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ及び証明装置用公開鍵データ１Ｂを記憶しておく。このうち、発行装置用秘密鍵データ２Ａ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃは各発行機関固有のものである。

【００２０】次に、図５に示すように、発行段階では、まず発行すべきカード４がカードリーダライタ２に挿入されると、カードリーダライタ２に設定された読み取り軌跡に沿って、基準領域４３から物理的特徴を信号として機械的に読み取り、特徴データ４Ｄとする。この特徴データ４Ｄを発行装置用秘密鍵データ２Ａを用いた署名生成ルールにより暗号化して発行装置署名データ４Ｃを生成する。そして、これら発行装置署名データ４Ｃ、特徴データ４Ｄ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ及び証明装置用公開鍵データ１Ｂをカード４の磁気ストライプ４２に格納する。

【００２１】次に、図６に示すように、認証装置としてのカードリーダ３による認証段階では、まず認証すべきカード４がカードリーダ３に挿入されると、磁気ストライプ４２に格納された発行装置署名データ４Ｃ、特徴データ４Ｄ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ及び証明装置用公開鍵データ１Ｂを読み出すと共にカードリーダ４に設定された読み取り軌跡に沿って、基準領域４３から物理的特徴を信号として機械的に読み取り、特徴データ４Ｄ′とする。

【００２２】そして、証明装置用公開鍵データ１Ｂを用いた署名検査ルールによって証明装置署名データ２Ｃを復号し、これを発行装置用公開鍵データ２Ｂと照合する。

【００２３】同様に発行装置用公開鍵データ２Ｂを用いた署名検査ルールによって発行装置署名データ４Ｃを復号し、これを特徴データ４Ｄと照合する。

【００２４】また、上記のように読み取った特徴データ４Ｄ′と特徴データ４Ｄとを照合する。

【００２５】上記各照合結果が所定の条件（各データ同士が一致、または不一致の程度が所定の範囲に収まっているなど）に一致したら、そのカード４が正規のカードであると判定する。

【００２６】図７、図８は、本発明が適用された第２の実施形態に於ける認証式セキュリティシステムに於けるカードの発行手順及び認証手順を説明する図であり、第１の実施形態に於ける図５、図６に対応する。このシステムも上記同様クレジットカードにおける認証式セキュリティシステムであり、その構成は第１の実施形態と概ね同様である。

【００２７】まず、準備段階としては上記同様にカードリーダライタ２に、発行装置用秘密鍵データ２Ａ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ及び証明装置用公開鍵データ１Ｂを記憶しておく。

【００２８】次に、図７に示すように、発行段階では、まず発行すべきカード４がカードリーダライタ２に挿入されると、カードリーダライタ２に設定された読み取り軌跡に沿って、基準領域４３から物理的特徴を信号として機械的に読み取り、そのデータ４Ｄを例えば１０分割して特徴データ４Ｄ１～４Ｄ１０とする。この特徴データ４Ｄ１～４Ｄ１０を発行装置用秘密鍵データ２Ａを用いた署名生成ルールにより暗号化して各々対応する発行装置署名データ４Ｃ１～４Ｃ１０を生成する。そして、これら発行装置署名データ４Ｃ１～４Ｃ１０、これに対応する特徴データ４Ｄ１～４Ｄ１０、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ及び証明装置用公開鍵データ１Ｂをカード４の磁気ストライプ４２に格納する。

【００２９】次に、図８に示すように、カードリーダ３による認証段階では、まず認証すべきカード４がカードリーダ３に挿入されると、磁気ストライプ４２に格納された発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ及び証明装置用公開鍵データ１Ｂを読み出すと共に発行装置署名データ４Ｃ１～４Ｃ１０及びこれに対応する特徴データ４Ｄ１～４Ｄ１０の中から認証の度に異なる１つまたは複数の発行装置署名データと特徴データとの組を読み出す。更にカードリーダ４に設定された読み取り軌跡に沿って、基準領域４３から物理的特徴を信号として機械的に読み取り、特徴データ４Ｄ′とする。

【００３０】そして、証明装置用公開鍵データ１Ｂを用いた署名検査ルールによって証明装置署名データ２Ｃを復号し、これを発行装置用公開鍵データ２Ｂと照合する。

【００３１】同様に、例えば今回の認証で発行装置署名データ４Ｃ５及びこれに対応する特徴データ４Ｄ５を読み出したとして、発行装置用公開鍵データ２Ｂを用いた署名検査ルールによって発行装置署名データ４Ｃ５を復号し、これを特徴データ４Ｄ５と照合する。

【００３２】また、特徴データ４Ｄ５と上記のように読み取った特徴データ４Ｄ′の対応部分とを照合する。

【００３３】上記各照合結果が所定の条件（各データ同士が一致、または不一致の程度が所定の範囲に収まって

いるなど）に一致したら、そのカード４が正規のカードであると判定する。

【００３４】この構成によれば、カードリーダ３による読み出し内容が認証の度に異なることから、両者間のデータ授受を傍受してもその解析、またはカードに格納されたデータを偽造カードに利用することは困難になる。また、この処理は従来カード（被認証物）側で複雑な処理を行っていた動的認証方法と同程度のセキュリティ性を実現しながら、カード側にはデータ格納領域を確保すれば良く、その構造が簡便化されると共にコストが低廉になっている。

【００３５】尚、上記構成では１つの特徴データを分割して複数の特徴データとしたが、基準領域４３の読み取り位置をずらして複数回読み取っても良い。

【００３６】図９、図１０は、本発明が適用された第３の実施形態に於ける認証式セキュリティシステムに於けるカードの発行手順及び認証手順を説明する図であり、第１の実施形態に於ける図５、図６に対応する。このシステムも上記同様クレジットカードにおける認証式セキュリティシステムであり、その構成は第１の実施形態と概ね同様であるが、カード４には磁気ストライプに代えてデータ記憶及び演算処理が可能なＩＣ４５及び接点（図示せず）が設けられ、カードリーダライタ２及びカードリーダ３には磁気ヘッドに代えてＩＣ４５の接点に接触するための対応接点（図示せず）が設けられている。カードリーダ３は、（疑似）乱数からなる確認データＲを生成するようになっている。また、ＩＣ４５は、被認証物用秘密鍵データ４Ａを用いて上記各実施形態と同様な署名生成ルールによりカードリーダ３側から送られる乱数からなる確認データＲを暗号化して被認証物署名データ４Ｃを生成するようになっている。

【００３７】まず、準備段階としては上記同様にカードリーダライタ２に、発行装置用秘密鍵データ２Ａ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ、証明装置用公開鍵データ１Ｂ、各カード４毎に設定される被認証者用秘密鍵データ４Ａ及び被認証者用公開鍵データ４Ｂを用意しておく。

【００３８】次に、図９に示すように、発行段階では、まず発行すべきカード４がカードリーダライタ２に挿入されると、カードリーダライタ２に設定された読み取り軌跡に沿って、基準領域４３から物理的特徴を信号として機械的に読み取り、特徴データ４Ｄとする。この特徴データ４Ｄを発行装置用秘密鍵データ２Ａを用いた署名生成ルールにより暗号化して発行装置署名データ４Ｃを生成する。そして、これら発行装置署名データ４Ｃ、特徴データ４Ｄ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ、証明装置用公開鍵データ１Ｂ、認証者用秘密鍵データ４Ａ及び被認証者用公開鍵データ４Ｂをカード４のＩＣ４５の記憶領域に格納する。

【００３９】次に、図１０に示すように、カードリーダ３による認証段階では、まず認証すべきカード４がカードリーダ３に挿入されると、ＩＣ４５の記憶領域に格納された発行装置署名データ４Ｃ、特徴データ４Ｄ、発行装置用公開鍵データ２Ｂ、証明装置署名データ２Ｃ、証明装置用公開鍵データ１Ｂ及び被認証者用公開鍵データ４Ｂを読み出すと共にカードリーダ３に設定された読み取り軌跡に沿って、基準領域４３から物理的特徴を信号として機械的に読み取り、特徴データ４Ｄ′とする。また、カードリーダ３側にて乱数を発生させ、これを確認データＲとしてＩＣ４５に送る。

【００４０】このとき、特徴データ４Ｄ′は疑似乱数でなく自然の乱数であることから、この一部やこれを何らかのアルゴリズムで処理したもの、或いは特徴データ４Ｄ′を抽出するのと同様な方法を用いて基準領域の一部や基準領域以外の領域から抽出したデータを確認データＲとして利用しても良い。これにより、疑似乱数の解析による乱数が特定されることを防止でき、セキュリティ性が一層向上する。所謂Ｆａｕｌｔ－ｂａｓｅｄ－ａｔｔａｃｋ等のように、ＣＰＵに対して外部から様々な刺激を与えることにより誤動作を起こさせるような攻撃方法も人為的な操作が介在する余地が殆どない方法によって発生した物理的な特徴を乱数として使用することにより防止できる。

【００４１】そして、証明装置用公開鍵データ１Ｂを用いた署名検査ルールによって証明装置署名データ２Ｃを復号し、これを発行装置用公開鍵データ２Ｂと照合する。

【００４２】同様に、発行装置用公開鍵データ２Ｂを用いた署名検査ルールによって発行装置署名データ４Ｃを復号し、これを特徴データ４Ｄと照合する。

【００４３】また、ＩＣ４５では確認データＲを被認証物用秘密鍵データ４Ａを用いた署名生成ルールにより暗号化して被認証物署名データ４Ｅを生成し、これをカードリーダ３側に送り返す。カードリーダ３では被認証物用公開鍵データ４Ｂを用いた署名検査ルールによって被認証物署名データ４Ｅを復号し、これを確認データＲと照合する。

【００４４】更に、特徴データ４Ｄと上記のように読み取った特徴データ４Ｄ′とを照合する。

【００４５】上記各照合結果が所定の条件（各データ同士が一致、または不一致の程度が所定の範囲に収まっているなど）に一致したら、そのカード４が正規のカードであると判定する。

【００４６】この構成によれば、上記同様カードリーダ３による読み出し内容が認証の度に異なることから、両者間のデータ授受を傍受してもその解析、またはカードに格納されたデータを偽造カードに利用することは困難になる。

【００４７】尚、上記各実施形態では被認証物に証明装置用公開鍵データ１Ｂを記憶させ、署名検査ルールによ

って証明装置署名データ２Ｃを復号し、これを発行装置用公開鍵データ２Ｂと照合したが、この処理は任意であり、例えば証明機関と発行機関とが同じ場合には省略することができる。また、証明機関が１つであり、その証明機関用秘密鍵データ１Ａ、証明機関用公開鍵データ１Ｂの変更がない場合、証明機関用公開鍵データ１Ｂは必ずしも被認証物側に記憶させておく必要はなく、認証装置製造時にこの認証装置に記憶させておいても良い。このようにすれば、独自に各秘密鍵データ、公開鍵データをも偽造しても証明機関用公開鍵データ１Ｂのみは正規なものを使わざるを得ないことから証明機関の秘密鍵データを知られない限り、上記照合が一致せず、チェックできることから、証明機関用秘密鍵データ及び公開鍵データの変更がないシステムの場合、そのメンテナンス性が低下することなくセキュリティ性が向上する。

【００４８】また、認証装置を、必要なときに証明装置と接続可能とし、かつ過去の認証時に被認証物から読み出された証明装置用公開鍵データを１つまたは２つ以上記憶可能とし、認証時に被認証物から読み出された証明装置用公開鍵データを記憶された証明装置用公開鍵データと比較し、一致すれば該証明装置用公開鍵データを用いて上記照合を行い、一致しなければ証明装置に通信等で問い合わせて正規の証明装置用公開鍵データであることが確認されたら該証明装置用公開鍵データを用いて照合を行うようにし、確認された該証明装置用公開鍵データを追加して記憶、または問い合わせ結果によっては変更するようにしても良い。この場合も独自に各秘密鍵データ、公開鍵データをも偽造しても証明機関用公開鍵データ１Ｂのみは正規なものを使わざるを得ないことから証明機関の秘密鍵データを知られない限り、上記照合が一致せず、チェックできる。従ってそのメンテナンス性が低下することなくセキュリティ性が向上する。更にこの構造では証明機関用秘密鍵データ及び公開鍵データが変更されても認証装置全てを同時に更新する必要はなく、認証時に新しい証明機関用公開鍵データが被認証物から読み出された場合にのみこれを追加して記憶、または新しいデータに置き換えれば良いことから証明装置用公開鍵データを認証装置にのみ記憶するシステムに比較してそのメンテナンス性が高くなっている。この認証装置のメンテナンス構造は、常にサーバと接続され、ＩＤや暗証番号、認証コードなどを確認するような端末機を有するシステムに一般的に単独で応用でき、サーバや接続回線の負荷が低減できるものである。

【００４９】また、上記各実施形態では被認証物をクレジットカードとしたが、例えばプリペイドカードやＩＤカード、固有の価値が証明された貴金属類、有価証券、部屋や自動車のキーなど、真正なものであることを証明する必要のあるものに任意に適用できることは云うまでもない。また、第１及び第２の実施形態では被認証物のデータ格納領域を磁気ストライプとしたが、第３の実施形態のようにＩＣチップをカードに埋め込んでＩＣカードとしても良い。

【００５０】

【発明の効果】このように、本発明によれば、人為的に同一なものを製作することが困難な基準領域の特徴データ、この特徴データを発行装置用秘密鍵データにより暗号化して生成された署名データ及び発行装置用公開鍵データを被認証物のデータ格納領域に格納しておき、これを認証時に読み出すと共にその基準領域の特徴を読み取り、これらの照合結果により被認証物の真正性を確認できるようにしたため、秘密鍵データを知らずに署名データを解析することは著しく困難であり、また被認証物のデータ格納領域に格納されたデータを単にデッドコピーしても他の被認証物では基準領域の特徴が異なることからその真正性は否定されるため他の被認証物への不正な適用をも効果的に防止することができ、しかも認証に必要なデータが全て被認証物側にあることから、認証装置側の記憶容量を著しく低減でき、また発行装置用秘密鍵データや発行装置用公開鍵データを変更したり新たな発行装置用秘密鍵データや発行装置用公開鍵データを追加しても認証装置側の更新を必要としないことからその保守が極めて簡便になる。

【００５１】特に、認証の度に被認証物と認証装置との通信内容を変えるようにする場合、請求項２のように被認証物側に格納された複数のデータの１つまたは幾つかを認証装置側で選択して読み出すようにすることで、被認証物側に演算処理のためのＩＣ等を設ける必要がなく、しかも処理が簡便になる。

【図面の簡単な説明】

【図１】本発明に基づくシステムの概略構成を示すブロック図。

【図２】本発明に基づくシステムが適用された記録媒体の一例としてのプリペイドカードを示す正面図。

【図３】プリペイドカードのためのカードリーダライタの一例を示すダイヤグラム図。

【図４】本発明に基づく第１の実施形態に於けるカードの作成手順を示すブロック図。

【図５】本発明に基づく第１の実施形態に於けるカードの作成手順を示すブロック図。

【図６】本発明に基づく第１の実施形態に於けるカードの認証手順を示すブロック図。

【図７】本発明に基づく第１の実施形態に於けるカードの作成手順を示すブロック図。

【図８】本発明に基づく第１の実施形態に於けるカードの認証手順を示すブロック図。

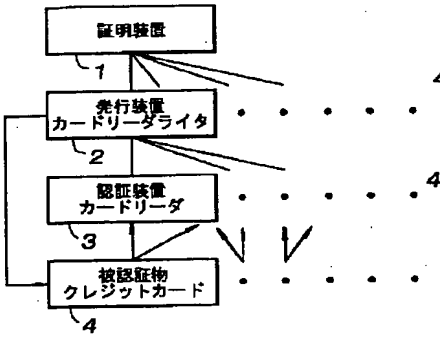
【図９】本発明に基づく第１の実施形態に於けるカードの作成手順を示すブロック図。

【図１０】本発明に基づく第１の実施形態に於けるカードの認証手順を示すブロック図。

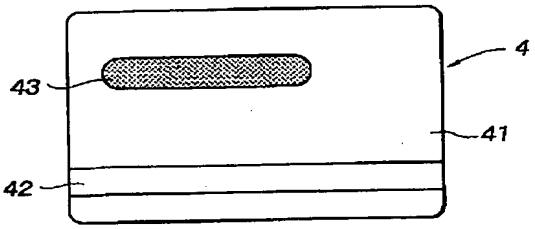
【符号の説明】

１　証明装置
２　カードリーダライタ（発行装置）
２１　スロット
２２　カード搬送ユニット
２３　磁気ヘッド
２４　誘導式磁気ヘッド
２５　制御ユニット
３　カードリーダ（認証装置）
４　クレジットカード（被認証物）
４１　ベースシート
４２　磁気ストライプ
４３　基準領域
４５　ＩＣ
１Ａ　証明装置用秘密鍵データ
１Ｂ　証明装置用公開鍵データ
２Ａ　発行装置用秘密鍵データ
２Ｂ　発行装置用公開鍵データ
２Ｃ　証明装置署名データ
４Ａ　被認証物用秘密鍵データ
４Ｂ　被認証物用公開鍵データ
４Ｃ　発行装置署名データ
４Ｃ１～４Ｃ１０　特徴データ４Ｄ１～４Ｄ１０に対応する発行装置署名データ
４Ｄ　特徴データ
４Ｄ′　認証時に読み取った特徴データ
４Ｄ１～４Ｄ１０　特徴データ４Ｄの分割データ
４Ｅ　被認証物署名データ
Ｒ　確認データ（乱数）

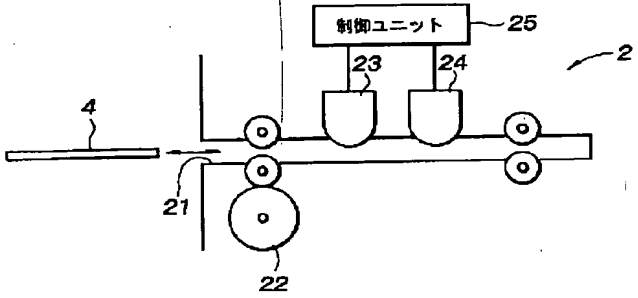
【図１】



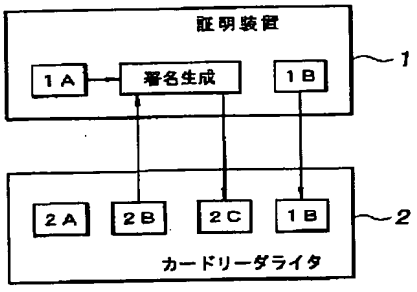
【図２】



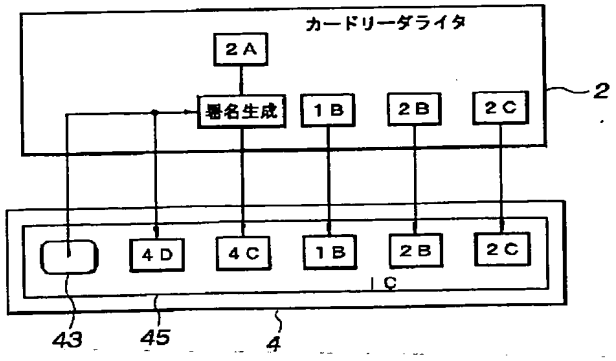
【図３】



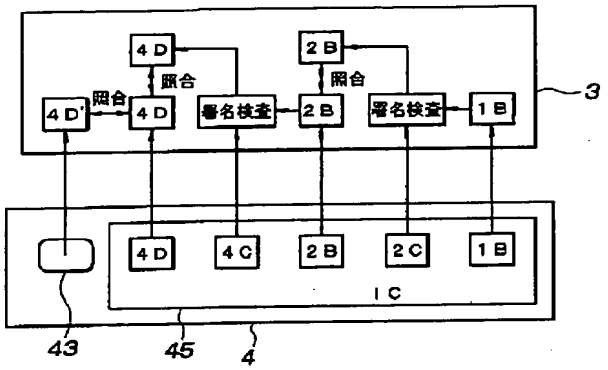
【図４】



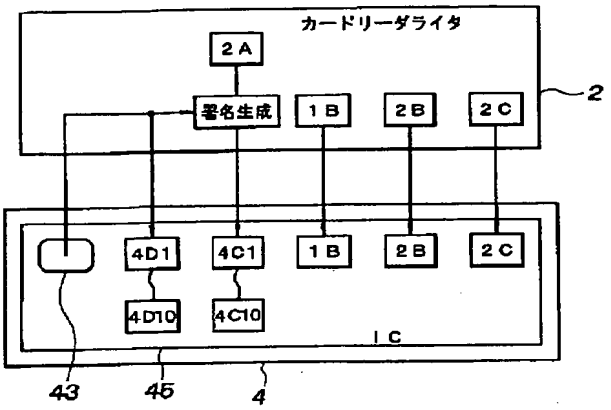
【図５】



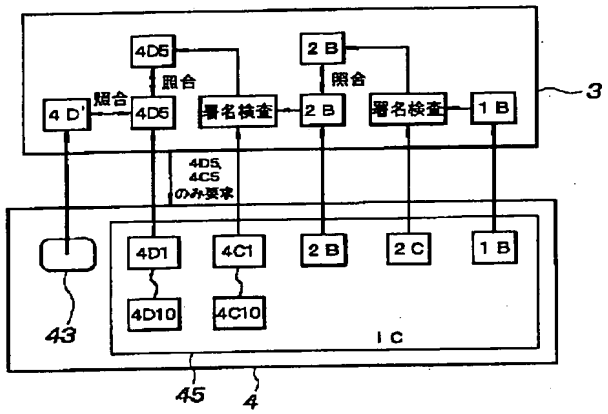
【図６】



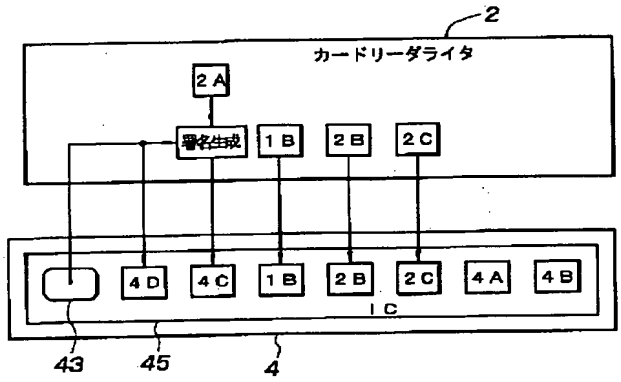
【図７】



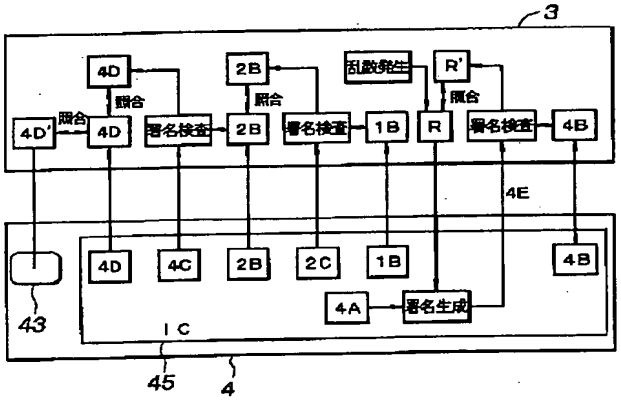
【図８】



【図９】



【図１０】



フロントページの続き

(72)発明者　山本屋　健二
神奈川県横浜市金沢区福浦３丁目10番地
日本発条株式会社内